SCIENTIA: Journal of Multi Disciplinary Sciences
Volume 02 Number 1 | Januari-Juni 2023: 15-27
p-ISSN: 2828-7665
e-ISSN: 2828-609X

PENGUATAN PENEGAKAN HUKUM POLRI DALAM RANGKA OPTIMALISASI PENANGGULANGAN *CYBERCRIME* DI INDONESIA

Ni Nyoman Putri Purnama Santhi[1)]* ; I Nengah Nuarta[2)]

[1)] putripurnama@iikmpbali.ac.id, **Program Studi Hukum, Universitas Bali Internasional, Indonesia**
[2)] nuarta@iikmpbali.ac.id, **Program Studi Hukum, Universitas Bali Internasional, Indonesia**
*) cooresponding author

Dikirim: 2023-01-26 Direvisi: 2023-02-23 Diterima: 2023-03-04

ABSTRAK

Penelitian ini mengkaji tentang bagaimana optimalisasi penanggulangan *Cybercrime* di Indonesia melalui penguatan penegakan hukum POLRI. Penelitian ini merupakan penelitian deskriptif di mana peneliti melakukan deskripsi terhadap informasi, data, serta fakta yang dihimpun dari studi pustaka seperti hasil penelitian, jurnal, dan buku yang relevan dengan topik penelitian. Penelitian ini memaparkan bahwasanya Perkembangan teknologi memegang peranan yang sangat kuat dalam memengaruhi perkembangan pelaku kejahatan. Sebelumnya, para penjahat mengimplementasikan cara-cara dengan menggunakan alat yang konvensional, akan tetapi sekarang, kejahatan dapat dilaksanakan menggunakan cara modern melalui internet yang disebut dengan *cybercrime*. Pemerintah telah membuat regulasi khusus terhadap *cyber law* yang diwujudkan menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Indonesia sangatlah membutuhkan penguatan hukum siber dalam rangka memperjuangkan ketahanan negara. Keberadaan hukum tersebut selain dapat memberikan perlindungan terhadap masyarakat sipil juga dapat memberikan perlindungan kepada negara dari ancaman kejahatan yang bisa terjadi pada dunia maya. Sebab itulah pemerintah menciptakan alat yang dapat digunakan untuk meningkatkan keyakinan dunia internasional mengenai keberadaan peraturan yang secara tegas meregulasi pertahanan siber sebagai usaha bela negara dalam rangka menciptakan keamanan global. Oleh karena itu, diperlukan Kerjasama berbagai pihak khususnya pemerintah, Polri dan masyarakat untuk memerangi kejahatan digital ini.

Kata kunci : kejahatan; digital; Polri.

ABSTRACT

This research examines how to optimize Cybercrime countermeasures in Indonesia by strengthening POLRI law enforcement. Descriptive research is research used by researchers in this study. Researchers describe facts, data, and information obtained from literature studies such as books, and journals to research results related to topics, and research. In this study, it was explained that technological developments have a strong influence on the development of criminals. In the past, crimes were committed using conventional means and tools, but now crimes are being committed in a modern way via the internet which is called Cybercrime. The government has made special regulations regarding cyber law which are embodied in Act Number of 19 of 2016 as the case changing of Act Number 11 of 2008 concerning Information and Electronic Transactions. Strengthening cyber law in Indonesia is very important, to fight for national defense. Not only protecting the community but also protecting nationally from the threat of Cybercrime. Then a component is created to convince the international community, about the existence of strict regulations in cyber defense as an effort to defend the country to build global security. Therefore, the cooperation of various parties, especially the government, POLRI, and the community is needed to fight this digital crime.

Keywords: *crime, digital, Polri.*

p-ISSN: 2828-7665
e-ISSN: 2828-609X

PENDAHULUAN

Kehidupan modern yang didukung oleh teknologi komunikasi memberikan kemudahan bagi masyarakat untuk menyerap dan berbagi berbagai informasi kepada individu maupun masyarakat (Rosmaladewi & Abduh, 2019). Dalam perkembangannya, penggunaan internet membawa banyak sisi negatif (Arianto & Anggraini, 2019). Hal ini meningkatkan peluang terjadinya tindak kriminal serta antisosial yang selama ini dinilai tidak mungkin terjadi. Sebagaimana disebutkan oleh sebuah teori bahwasanya sebuah kejahatan ialah produk yang tercipta dari sekelompok masyarakat. Artinya, masyarakat ialah pihak yang bertanggungjawab atas terciptanya suatu kejahatan. Tingginya tingkat intelektual yang dimiliki masyarakat akan diiringi pula dengan tingginya kecanggihan tindak kriminal yang dapat terjadi di masyarakat (Alghamdi, I, 2020). Permasalahan terkait keamanan sangatlah esensial di internet, karena minimnya keamanan akan meningkatkan risiko pencurian data yang terdapat dalam sistem internet oleh pihak-pihak yang tidak bertanggung jawab. Sebuah sistem jaringan berbasis internet seringnya mempunyai kelemahan yang kerap disebut sebagai "lubang keamanan". Pencuri tentunya dapat dengan mudah memasuki lubang bilamana tidak dilakukan penutupan terhadapnya. Tentunya, pencurian data dalam suatu sistem di internet dapat disebut sebagai kasus kejahatan komputer. "*Cybercrime"* ialah frasa yang sering digunakan dalam mendeskripsikan kejahatan yang terjadi di internet (Sarre et al., 2018).

Di Indonesia masalah cybercrime telah menjadi perhatian baik masyarakat maupun pemerintah, sebelumnya UU ITE yang meregulasi mengenai *cybercrime* secara khusus belum ada, sehingga masalah cybercrime ditindaklanjuti dengan undang-undang yang relevan dengan permasalahan itu. Tetapi kini kasus cybercrime telah diregulasi oleh UU ITE (Saleh, 2022). Kasus cybercrime telah diregulasi dalam UU ITE Nomor 8 Tahun 2011 dan selanjutnya dihadapkan pada perubahan Undang-Undang Nomor 19 Tahun 2016, khususnya pada pasal 27-30 terkait dengan perilaku yang tidak dianjurkan untuk dilakukan di dunia maya (Arwana, 2022). Kejahatan di dunia maya tidak dapat dihindari meskipun telah dibuat undang-undang yang mengaturnya, namun setiap tahun kasus kejahatan dunia maya di Indonesia semakin meningkat. Masyarakat diharapkan lebih bijak dalam menyikapi perkembangan teknologi yang ada, sehingga bilamana ingin menyebarkan data pribadi, masyarakat hendaknya melakukannya dengan penuh kehati-hatian. Sebab perkembangan teknologi informasi tidak hanya memberikan pengaruh positif tetapi juga negative (Rahmat et al., 2022).

Sebuah kasus *cybercrime* yang pernah ada di Indonesia salah satunya ialah kasus Steven Haryanto di tahun 2001 di mana ia membobol internet banking Bank Central Asia (BCA). Menarik untuk disimak, ketika pelaku salah ketik *clickbca.com* sehingga ia sukses melaksanakan rencana jahatnya dengan mencatat 130 *Personal Identification Number* (PIN) beserta *user ID* Nasabah Bank *Central Asia*, hanya meminta maaf pada pihak Bank BCA karena dianggap tidak melakukan tindakan kriminal dan hanya dibuat atas dasar menguji tingkat keamanan sistus tersebut (Mashdurohatun et al., 2017). Kasus lain yang sering terjadi terkait cybercrime saat ini adalah maraknya serangan *ransomware.* Pada Mei 2021 adalah salah satu insiden cyber paling berdampak dalam beberapa tahun terakhir yakni serangan *ransomware* DarkSide terhadap *Colonial Pipeline* operator pipa bahan bakar terbesar di AS. Segera setelah serangan itu,

p-ISSN: 2828-7665
e-ISSN: 2828-609X

pemerintah AS terpaksa mengumumkan keadaan darurat dan Departemen Perhubungan untuk sementara melonggarkan peraturan di sebagian besar Atlantik Tengah dan AS bagian selatan, serta Texas, yang mengatur berapa lama pengemudi truk diizinkan untuk tetap berada di belakang kemudi, untuk meningkatkan fleksibilitas dalam rantai pasokan bahan bakar (Keary, 2022).

Sisi gelap dari internet meningkatkan urgensi keamanan siber (Rizal & Yani, 2016). Sehingga diperlukan kerjasama dari beberapa pihak terkait khususnya Polri sebagai pihak yang memiliki tugas memberi keamanan dan ketentraman dalam menyelesaikan permasalahan ini. Berdasarkan permasalahan yang telah diuraikan, dalam menghadapi maraknya cybercrime, diperlukan profesionalisme yang tinggi dari aparat kepolisian. Hal ini dapat diwujudkan dengan terus meningkatkan kualitas sumber daya POLRI baik secara kuantitas maupun kualitas (Maltha et al., 2019). Dengan demikian perlu dirumuskan dalam penelitian ini yakni penguatan penegakan hukum POLRI dalam rangka optimalisasi penanggulangan cybercrime di Indonesia.

TINJAUAN PUSTAKA

Penegakan Hukum

Penegakan hukum ialah sebuah upaya dalam merealisasikan kebermanfaatan sosial, kepastian hukum, serta ide-ide keadilan, sehingga pada hakikatnya penegakan hukum ialah sebuah proses untuk mewujudkan ide. Adapun penegakan hukum menurut Faridah (2018) ialah proses pengimplementasian usaha fungsinya/tegaknya norma hukum secara *riil* sebagai dasar tingkah laku dalam berlalu lintas maupun hubungan hukum lainnya dalam kehidupan bernegara serta bermasyarakat. Penegakan hukum ialah upaya dalam merealisasikan konsep serta ide hukum yang diharapkan oleh masyarakat, di mana dalam pelaksanaannya tentunya akan sangat melibatkan banyak hal.

Kesuksesan penegakan hukum sangat dipengaruhi oleh faktor-faktor yang maknanya netral, sebab itulah efek positif dan negatifnya sangat bergantung pada komponen dari faktor tersebut. Faktor ini sangat berkaitan antar satu dengan yang lain di mana hal tersebut menjadi parameter serta esensi efektivitas penegakan hukum. Adapun faktor yang berkorelasi dengan penegakan hukum antara lain ialah komponen struktur, substansi dan kultur. Menurut (Arliman. S, 2019) negara hukum menjadikan penegakan hukum sebagai pokoknya, sebab hal tersebut adalah cerminan dari suatu negara. Negara hukum yang baik dapat terlihat dari perwujudan penegakan hukumnya sehingga tentunya, warga negara hukum tersebut akan merasa nyaman di dalamnya.

Penegakan hukum ialah upaya merealisasikan konsep serta ide hukum yang diharapkan oleh rakyat. Dalam prosesnya, penegakan hukum akan sangat melibatkan banyak aspek. Setiawan et al (2020) menyatakan bahwasanya sejatinya penegakan hukum secara konteks luas termasuk dalam ranah perilaku, perbuatan, maupun tindakan yang faktual/nyata yang selaras dengan norma beserta kaidah yang mengikat. Akan tetapi, dalam usaha memulihkan serta menjaga ketertiban kehidupan sosial, maka pemerintah bertindak sebagai *actor security.*

Secara konkret, penegakan hukum ialah keberlakuan hukum positif dalam realisasinya sebagaimana seharusnya diimplementasikan. Sebab itulah, pemberian keadilan pada sebuah perkara bermakna memutuskan hukum *in concreto* dalam

p-ISSN: 2828-7665
e-ISSN: 2828-609X

menjamin serta mempertahankan ketaatan terhadap hukum materiil melalui mekanisme prosedural yang telah diatur dalam hukum formal (Wicaksono & Najicha, 2021). Penegakan hukum bisa diimplementasikan oleh subjek luas dan bisa diinterpretasikan sebagai usaha penegakan hukum yang dilakukan subjek dalam makna yang sempit/terbatas. Adapun pada makna yang luas, proses dalam penegakan hukum tersebut melibatkan seluruh subjek hukum pada seluruh hubungan hukum. Semua pihak yang mengimplementasikan aturan normatif, baik melaksanakan ataupun tidak melaksanakan sesuatu dengan berpedoman pada norma aturan hukum yang berlaku dapat dikatakan bahwasanya ia sedang mengimplementasikan/menegakkan aturan hukum. Adapun menurut makna sempitnya, berdasarkan subjek penegakan hukum tersebut sebatas dimaknai sebagai usaha aparat penegak hukum dalam memberikan kepastian dan jaminan bahwasanya sebuah aturan hukum telah terimplementasikan seperti yang seharusnya. Bilamana diperlukan, maka aparat penegak hukum dalam mempergunakan daya paksa untuk benar-benar memastikan hukum yang berlaku ditegakkan.

Cybercrime

Dalam membahas mengenai *cybercrime,* peneliti juga akan turut membahas mengenai keamanan sebuah jaringan komputer maupun informasi teknologi telekomunikasi. Pesatnya perkembangan teknologi di era globalisasi saat ini tentunya turut meningkatkan risiko penyalahgunaan dari pemanfaatan teknologi yang kini dibutuhkan sebagai sumber informasi. Pesatnya perkembangan teknologi tersebut dapat memberikan dampak yang luar biasa bagi peradaban manusia, baik berupa dampak negatif maupun positif. Menurut (Apriani et al., 2019, teknologi komputer yang signifikan perkembangannya kini menjadi kebutuhan dalam meningkatkan mutu layanan terhadap pelanggan.)

Manusia dapat memanfaatkan kemajuan teknologi dan informasi ini sebagai komoditi informasi. Namun di sisi lain, pesatnya perkembangan tersebut bisa disalahgunakan yang mengarah pada tindak pidana *cybercrime*. Sejauh ini, pesatnya perkembangan teknologi informasi dan komputer sukses memberikan pengaruh terhadap aktivitas serta pola kerja masyarakat. Menurut (Chanda Halim & Hendri Prasetyo, 2018), tindak pidana cybercrime mempunyai karakteristik/ciri khas khusus yang membuat penanganan terhadapnya pun juga harus dibedakan dari tindak pidana konvensional.

Cybercrime ialah frasa yang dapat digunakan dalam mendeskripsikan kegiatan kejahatan yang menjadikan jaringan komputer/komputer sebagai tempat kejadian, sasaran, maupun alat kejahatan. Di antara peristiwa yang dapat dikategorikan sebagai *cybercrime* antara lain ialah penipuan identitas, *carding/*penipuan kartu, penipuan lelang secara daring, pornografi anak, *confidence fraud,* serta pemalsuan cek. (Chanda Halim & Hendri Prasetyo, 2018) menyatakan bahwasanya *cybercrime* ialah perkembangan bentuk kejahatan yang terjadi pada *real space*, adapun *cyber warfare* ialah perkembangan dari bentuk perang yang terjadi pada *real space*. Selanjutnya, *cyber attack* didefinisikan secara berbeda dari kedua istilah sebelumnya. Perbedaan definisi antara ketiga hal tersebut sangatlah esensial sebab dapat memicu konsekuensi hukum yang berbeda dan tentunya, hal tersebut akan diregulasi oleh hukum yang juga berbeda.

p-ISSN: 2828-7665
e-ISSN: 2828-609X

Cybercrime ialah bentuk kejahatan yang kemunculannya diakibatkan oleh pemanfaatan internet. Menurut (Abidin, 2015) definisi dari cybercrime ialah perilaku melawan hukum yang pelaksanaannya digunakan menggunakan objek berupa komputer dan alat/sarana berupa jaringan komputer baik dalam rangka mendapatkan keuntungan maupun tidak akan tetapi perilaku tersebut bisa memberikan dampak kerugian bagi pihak lainnya. Cybercrime dapat diklasifikasikan menjadi beberapa jenis berdasarkan sasaran kejahatannya, motif kegiatannya, serta aktivitas yang dilakukannya.

Indonesia telah memiliki hukum berupa undang-undang yang secara khusus mengatur mengenai kejahatan dunia maya, yakni Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE) yang mengkaji mengenai batasan dan tata cara penggunaan komputer beserta hukuman atas pelanggaran terhadapnya. Salah satu hal tersebut contohnya, tindakan *illegal access* di mana pelaku melakukan akses secara ilegal/tidak sah. Tindakan tersebut telah diregulasi pada pasal 30 UU ITE yang menyatakan, "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses komputer dan/atau sistem elektronik milik orang lain ayat (1)) dengan cara apapun, (ayat (2)) dengan cara apa pun dengan tujuan untuk memperoleh informasi elektronik dan/atau dokumen elektronik, (ayat (3)) dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol system pengaman".

Penelitian Terdahulu

Penelitian yang pernah dilakukan oleh (WIJATMOKO, 2021) dengan judul penelitian "Digital Forensik Readlines Index (DIFRI) untuk Mengukur Kesiapan Penanggulangan Cybercrime Pada Kantor Wilayah Kementerian Hukum dan HAM DIY". Penelitian tersebut bertujuan dalam rangka mengetahui bagaimana kesiapan Kantor Wilayah Kementerian Hukum dan Hak Asasi Manusia DIY dalam menghadapi cybercrime sehingga harapannya, pembenahan serta perbaikan yang dilakukan bisa tepat sesuai sasaran. Data yang dihimpun dari kuesioner lalu dianalisis menggunakan metode statistik. Penelitian tersebut menemukan bahwasanya lembaga pemerintah dinilai memiliki kesiapan yang cukup dalam menghadapi *cybercrime* dan diharapkan mampu melaksanakan perbaikan beserta pembenahan yang tepat sasaran supaya di masa depan, aset informasi dapat terlindungi dari usaha-usaha pelaksanaan tindak kejahatan.

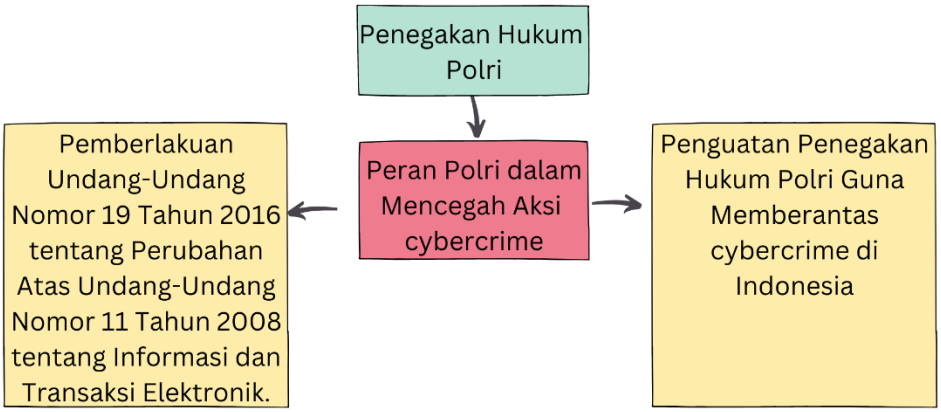
Penelitian yang dilakukan oleh (Raodia, 2019) pada tahun 2019 dengan judul penelitian "Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (cybercrime)" dengan tujuan penelitian guna mengetahui bagaimana perkembangan teknologi memengaruhi terjadinya kejahatan mayantara. Penelitian ini menemukan bahwasanya cara yang dapat dilaksanakan untuk menanggulangi serta mencegah kejahatan mayantara antara lain ialah: 1) Menyusun regulasi/undang-undang yang secara khusus meregulasi mengenai kejahatan mayantara, dan 2) Meningkatkan kualitas sumber daya manusia yang menjadi aparat penegak hukum serta di lembaga kepolisian.

Penelitian yang dilakukan oleh (Putra, 2016) dengan judul penelitian "Analisis Hukum Yurisdiksi Tindak Kejahatan Siber (cybercrime) Berdasarkan *Convention on Cybercrime*" pada tahun penelitian 2016 dengan tujuan penelitian untuk mengetahui pengaturan yurisdiksi cybercrime beserta bentuk konkret kerjasama antarnegara dalam

p-ISSN: 2828-7665
e-ISSN: 2828-609X

menanggulangi cybercrime dengan berpedoman pada *Convention on Cybercrime*. Penelitian ini ialah penelitian yuridis normatif dengan *conceptual approach.* Peneliti menggunakan bahan hukum primer berupa peraturan perundangan yang relevan dengan topik penelitian, bahan hukum sekunder berupa jurnal, literatur, serta buku yang relevan, serta bahan hukum tersier meliputi buku pegangan, kamus umum blibliography, serta ensiklopedia yang diterbitkan oleh pemerintah yang didalamnya menjelaskan mengenai pengertian, konsep, beserta istilah dari bahan hukum lainnya. Penelitian ini menemukan bahwasanya regulasi mengenai yurisdiksi dalam hukum internasional khusus mengenai cybercrime telah diregulasi oleh *Convention on Cybercrime.* Permasalahan yurisdiksi dalam *Convention on Cybercrime* yang disusun Dewan Eropa, secara khusus ditempatkan pada Pasal tersendiri yakni Pasal 22. Bilamana konflik yurisdiksi terjadi, maka negara dapat melakukan cara kerjasama internasional sebagai penyelesaiannya, meliputi: a. *Transfer of Proceeding,* b. *Mutual Legal Assistance/*bantuan timbal-balik, dan c. Deportasi dan Ekstradisi.

Gambar 1 Kerangka Teoritis



METODE

Penelitian yang dilakukan penulis ini masuk ke dalam penelitian kualitatif deskriptif. Penelitian kualitatif deskriptif ini didapatkan dari berbagai sumber diantaranya adalah buku, artikel dan jurnal penelitian serta beberapa bahan literatur lainnya (Afrizal, 2016). Disamping itu, penulis juga melakukan pengkritisian dan pengkajian gagasan, temuan ilmiah serta pengetahuan yang berkontribusi positif pada perkembangan ilmu pengetahuan dan orientasi akademik. Tidak hanya itu, temuan penelitian nantinya diharapkan bisa berkontribusi serta memberi manfaat yang positif baik jika ditinjau dari metodologi pada tema yang dikaji oleh penulis maupun secara teori yang digunakan untuk menjelaskan beberapa isu, fenomena serta fakta dialami oleh masyarakat (Arikunto, 2010). Fakta serta data tersebut kemudian akan dilakukan pengembangan oleh penulis untuk dikumpulkan menjadi informasi yang berhubungan dengan tema penelitian yang dikaji penulis.

p-ISSN: 2828-7665
e-ISSN: 2828-609X

HASIL DAN PEMBAHASAN

Peran POLRI dalam Mencegah Aksi Cybercrime

Kemajuan era globalisasi dan kemajuan teknologi dalam penyebaran informasi telah menjadi fakta bahwa arus revolusi industri tidak dapat dibendung dan terus mengalami kemajuan. Pilihan terbaik adalah merespons aliran ini dengan baik. Kejahatan dunia maya membutuhkan perhatian serius bagi siapa pun; adanya perilaku menyimpang dari sekelompok orang atau individu yang menggunakan teknologi dan dunia maya untuk melakukan kejahatan demi keuntungan pribadi cenderung menimbulkan kerugian bagi pihak lain. Pemahaman dan pengetahuan akan pentingnya perlindungan data merupakan salah satu hal yang harus terus ditingkatkan pemerintah dengan segala upaya, baik melalui peraturan perundang-undangan maupun pembinaan langsung melalui sosialisasi kepada masyarakat. Sebuah upaya yang perlu diapresiasi dan harus terus dimaksimalkan. Namun di sisi lain, sudah seharusnya masyarakat waspada dan mengontrol perilakunya di internet karena saat ini jari kita bisa melakukan apa saja, dan bisa apa saja di dunia maya, baik itu hal yang positif maupun yang berdampak negatif bagi kehidupan. diri mereka sendiri dan orang lain. Elaborasi antara masyarakat dan organ pemerintah harus berjalan beriringan untuk menciptakan keamanan dan kenyamanan berinternet.

Media elektronik tidak dapat disangkal memang memfasilitasi aktivitas masyarakat global dan salah satunya dalam transaksi bisnis, terutama bisnis keuangan di samping bisnis lainnya. Bertepatan dengan kemajuan teknologi dan informasi publik dibuat untuk mengikuti semua perkembangan yang terjadi. sedang terjadi (Sugiharti et al., 2022). Dalam berkomunikasi dan bersosialisasi sangat diperlukan kemajuan teknologi dan informasi, karena hal tersebut memudahkan masyarakat dalam segala hal, yaitu berkomunikasi dengan cara baru, berjualan dengan cara baru, dan berbisnis tanpa batasan waktu dan tempat (Sakban et al., 2020). Hal ini membuka mata masyarakat dengan dunia baru yang perkembangannya sangat pesat. Internet merupakan salah satu metode yang sangat sering digunakan dalam hal ini karena internet merupakan salah satu perkembangan teknologi yang telah mengubah dunia dari tahun ke tahun (Damayanti & Ismowati, 2021).

Cybercrime yang dilakukan dengan cara menyusup ke sistem jaringan komputer secara ilegal, tanpa izin atau sepengetahuan pemilik sistem jaringan komputer dimasukkan (Sugiartha et al., 2021). Biasanya, pelaku (cracker) menyabotase atau mencuri informasi berharga dan rahasia. Namun, ada pula yang melakukannya hanya karena merasa tertantang untuk mencoba keahliannya menembus sistem yang memiliki tingkat proteksi tinggi. Kejahatan lebih banyak terjadi dengan perkembangan teknologi internet/intranet dibandingkan masa lalu (Mandasari Saragih & Utama Siahaan, 2016). Di Indonesia, kejahatan siber sulit dinyatakan atau dikategorikan karena asas legalitas. Dalam kejahatan siber (menggunakan internet), posisi Indonesia telah menggantikan Ukraina yang sebelumnya menduduki posisi pertama. Kejahatan internet (cybercrime) yang marak di Indonesia antara lain penipuan kartu kredit, penipuan perbankan, deface, cracking, hacking, transaksi seks, perjudian online, terorisme dengan korban yang berasal dari dalam negeri dan luar negeri seperti AS, Inggris, Australia, Jerman, Korea, dan Singapura, serta beberapa wilayah di negara ini (Rais & Songkarn, 2022).

Dalam lingkup domestik, upaya yang dilakukan POLRI dalam menanggulangi terjadinya cybercrime telah dilakukan beberapa upaya yaitu:

1. Menanggapi dan menerima setiap laporan dari masyarakat atas dugaan kejahatan dunia maya dan mencatat setiap kasus yang ditangani terhadap laporan tersebut.
2. Melakukan investigasi online (melalui internet/virtual) terhadap kejahatan dengan menggunakan jejaring sosial, email dan e-commerce.
3. Berkoordinasi dengan Kementerian Komunikasi dan Informatika
4. Bekerja sama di bidang perbankan, khususnya dengan Bank Indonesia, untuk menghindari rekening palsu yang digunakan oleh penjahat.
5. Kami mengimbau masyarakat untuk selalu menggunakan internet secara aman.
6. Meningkatkan pemahaman dan pelatihan keahlian POLRI di bidang cybercrime dengan mengirimkan anggotanya untuk pelatihan dan kursus di beberapa negara maju (Arianto & Anggraini, 2019).

Di samping itu, beberapa upaya penanggulangan yang dapat dioptimalissasikan oleh POLRI yang ditawarkan oleh Conteh dan Schimck diantaranya adalah berupa:

1. Kebijakan Keamanan: Kebijakan yang ditulis dengan baik harus mencakup pendekatan teknis dan nonteknis yang didorong ke bawah oleh manajemen eksekutif. Setiap organisasi harus mengintegrasikan keamanan ke dalam tujuan operasional mereka.
2. Pendidikan dan Pelatihan: Karyawan harus diwajibkan agar mengikuti pelatihan awal selama orientasi dan pelatihan penyegaran berulang. Ini membangun kesadaran dengan memaparkan pengguna pada taktik dan perilaku yang umum digunakan yang dikorbankan oleh seorang insinyur sosial.
3. Panduan Jaringan: Organisasi harus melindungi jaringan dengan memasukkan situs web resmi ke daftar putih, menggunakan Terjemahan alamat jaringan (NAT), dan menonaktifkan aplikasi dan port yang tidak digunakan. Pengguna jaringan harus mempertahankan kata sandi kompleks yang diubah setiap 60 hari.
4. Audit dan Kepatuhan: Organisasi harus secara aktif memverifikasi bahwa kebijakan keamanan mereka dipatuhi. Beberapa kontrol detektif termasuk meninjau log jaringan, memvalidasi ulang izin karyawan, dan memeriksa konfigurasi desktop setidaknya dua bulanan.
5. Prosedur Teknis: Jaringan harus memiliki beberapa lapisan pertahanan agar melindungi data dan infrastruktur inti. Perangkat lunak seperti *Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS)* dan firewall harus dipasang di setiap perangkat. Zona Demiliterisasi (DMZ), filter web, dan *Virtual Private Network* (VPN) harus dipasang di semua layanan eksternal (Darmaningrat et al., 2022).

Berdasarkan cara penanggulangan demikian maka ini sudah kucup memenuhi visi POLRI yang dikatakan bahwa Polri prediktif, responsibilitas, dan transparansi. Hal ini tentu dengan beberapa catatan berupa bahwa keprofesionalitasan ini diterapkan dalam berbagai kasus tidak dalam hal ini saja. Penjabarannya dalam presisis memuat tiga poin berharga yaitu prediktif, responsibilitas, dan transparansi. Maka dapat diketahui secara prediktif POLRI dalam menanggulangi kasus demikian maka dapat mengoptimalkan upaya prosedur teknis dan panduan fisik. Hal ini dikarenakan bahwa memprediksi masalah seperti ini butuh adanya pengkajian lebih bukan serta merta memvonis bahwa

p-ISSN: 2828-7665
e-ISSN: 2828-609X

hal lain berupa kejahatan *social engineering.* Lebih lanjut dalam responsibilitas terhadap kasus demikian maka dapat dioptimalkan agar sosialisasi dan edukasi ke masyarakat selain itu juga menetapkan beberapa kebijakan bersama pemerintahan guna memeprkuat kemanaan.

Penguatan Penegakan Hukum POLRI Guna Memberantas Cybercrime di Indonesia

Dalam prakteknya, Polri harus profesional dan selalu siap menghadapi setiap gejala yang ada di masyarakat serta harus mampu menjadi lembaga yang fleksibel dengan mengikuti perkembangan zaman dan menyesuaikannya. Secara sosiologis, akan selalu berkaitan dengan kedudukan, sehingga pemahaman peran Polri tidak dapat dipisahkan dari posisinya dalam sistem ketatanegaraan yang dianut. Dalam sistem demokrasi, fungsi polisi dapat dikelompokkan menjadi tiga fungsi yang menuntut karakter dan cara bekerja sama satu sama lain: memerangi kejahatan, melindungi warga negara dan menjaga ketertiban umum. Dari fungsi kepolisian tersebut, 4 (empat) peran harus dijalankan yaitu peran aparat penegak hukum, peran menjaga ketertiban peran petugas perdamaian, dan peran. Keempat peran tersebut bermuara pada output melindungi dan melayani sehingga polisi sebagai penjaga nilai-nilai kemasyarakatan dalam iklim kehidupan demokrasi dapat terwujud (Damayanti & Ismowati, 2021).

Salah satu pembentukan *cyber police* dimulai dengan mengeluarkan surat edaran dari KAPOLRI yaitu SE No. SE/2/11/2021 tentang Kesadaran Budaya Etis untuk Mewujudkan Ruang Digital Indonesia yang Bersih, Sehat, dan Produktif. SE tersebut merupakan keputusan untuk menindaklanjuti permintaan Presiden agar POLRI lebih selektif dalam menangani kasus dugaan pelanggaran UU ITE*. Cyber police* melakukan kegiatan *cyber patrol* dengan memantau setiap kegiatan di dunia maya terutama melalui media sosial dan berbagai platform lainnya (Rais & Songkarn, 2022).

Polisi sebagai lembaga yang menjembatani hal tersebut juga tidak lelah untuk terus bekerja dan memberikan inovasi dalam menghadapi setiap gejala dan fenomena di masyarakat. Dengan hadirnya *cyber police* diharapkan mampu menciptakan kenyamanan dalam menggunakan sosial media dan *platform* lainnya. Di saat yang sama, POLRI terus memantau dan melatih anggotanya untuk memberikan sikap preventif dalam menangani kasus-kasus yang terjadi di dunia maya. Dengan demikian, dapat dikatakan bahwa *cyber police* tidak hanya bertugas menangani pengaduan atau laporan masyarakat tetapi juga melakukan pencegahan melalui sosialisasi dan *cyber public relation* untuk memastikan masyarakat mendapatkan informasi yang baik dan mencegah beredarnya hoaks. Semoga hal ini terus berkembang dan memberikan manfaat lebih bagi masyarakat luas.

Selain itu, dalam mengusut kejahatan dunia maya yang berkaitan dengan komentar jahat, pencemaran nama baik dan hoax, terutama yang mengganggu kepentingan nasional, POLRI cukup agresif. UU ITE, Peraturan Pemerintah 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Menteri Komunikasi dan Informatika (PERMENKOMINFO) 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (bersama-sama disebut Peraturan PDP) melakukan privasi atau data hukum perlindungan. Jika tidak ada standar khusus, untuk dapat diduga adanya pelanggaran terhadap undang-undang privasi atau perlindungan data, regulator terikat dengan standar berdasarkan hukum pidana yang

berlaku di Indonesia. Hukum pidana Indonesia mensyaratkan regulator untuk mengajukan minimal dua bukti untuk menetapkan dugaan pelanggaran pidana (Suhendi & Asmadi, 2021).

Mengacu pada ciri tersebut, maka seorang penegak hukum hendaknya mengikuti prosedur serta berhati-hati ketika sedang berhadapan dengan barang bukti elektronik supaya keutuhan dari barang elektronik tersebut tidak mengalami perubahan. Regulasi teknik terkait tata cara penanganan barang bukti elektronik yang digunakan oleh aparat penegak hukum di Indonesia kini didasarkan pada Peraturan Kapolri Nomor 10 Tahun 2009 tentang Tata Cara dan Persyaratan Permohonan Pemeriksaan Teknis Pidana di Tempat Perkara dan Laboratorium Bukti Kriminal menjadi Laboratorium Forensik (disebut PERKAP 10/2009) (Hartati et al., 2022). Secara umum beberapa aturan yang telah dijabarkan terkait dengan kejahatan cybercrime ini tercantum dalam UU ITE yang disusun pada Maret 2003 oleh Kementerian Negara Komunikasi dan Informatika yang diubah menjadi Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Anggraeny et al., 2022). Secara garis besar, UU ITE ini mengatur:

1. Tanda tangan elektronik mempunyai kekuatan hukum yang sama dengan tanda konvensional (tinta basah dan stempel). Sesuai dengan Pedoman Kerangka Kerja e-ASEAN (pengakuan tanda tangan digital lintas batas).
2. Alat bukti elektronik diakui sebagai alat bukti lain yang diatur dalam KUHP.
3. UU ITE berlaku bagi setiap orang yang melakukan perbuatan hukum, baik di Indonesia maupun di luar Indonesia yang menimbulkan akibat hukum di Indonesia.
4. Pengaturan Nama Domain dan Hak Kekayaan Intelektual.
5. Perbuatan yang dilarang yakni cybercrime dan dijelaskan pada Bab VII (Pasal 27-37) (Manihuruk & Tarina, 2020).

Dari uraian di atas dapat dipahami bahawa UU ITE terlahir guna meregulasi pesatnya kemajuan dan perkembangan teknologi. Efek yang dihasilkan dari berkembangnya teknologi itu salah satunya ialah menempatkan manusia dlaam ruang komunikasi yang *borderless* (Hartati et al., 2022).

KESIMPULAN

Pemerintah telah membuat regulasi khusus mengenai *cyberlaw* yang diwujudkan menjadi Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Masyarakat Indonesia telah diserahkan oleh penyebaran berita *hoax* yang mengakibatkan banyak masyarakat menjadi mudah terprovokasi dengan sebaran informasi/berita yang tidak bisa dipertanggungjawabkan kebenarannya tersebut. Kebutuhan untuk memilih serta memahami berita yang aktual guna dikirimkan lagi pada pihak lainnya. Penguatan hukum siber di Indonesia sangat penting dalam rangka untuk memperjuangkan pertahanan negara. Sebab itulah, hal tersebut menjadi tanggung jawab bersama antara para subjek yang berkepentingan, yakni pemerintah, aparat penegak hukum dalam hal ini khususnya Polri, serta seluruh elemen masyarakat untuk memerangi gejolak cybercrime. Adapun landasan penegakan hukum yang bisa memberikan jawaban atas tuntutan masyarakat adalah hukum yang responsif yang

dimana bertujuan untuk melahirkan semangat keadilan beserta moralitas yang menjadi cita hukum. Reformasi hukum hendaknya kembali melihat kepada kekuatan moralitas yang berkembang, tumbuh, serta hidup di antara masyarakat.

REFERENSI

Abidin, D. Z. (2015). Kejahatan dalam Teknologi Informasi dan Komunikasi. *Jurnal Ilmiah Media Processor*, *10*(2).

Afrizal. (2016). *Metode Penelitian Kualitatif: Sebuah Upaya Mendukung Penggunaan Penelitian Kualitatif Dalam Berbagai Disiplin Ilmu*. PT. Raja Grafindo Persada.

Alghamdi, I, M. (2020). A Descriptive Study on the Impact of *Cybercrime* and Possible Measures to Curtail its Spread Worldwide. *International Journal of Engineering Research Technology*, *09*(06), 1321–1330.

Anggraeny, I., Monique, C., Puspitasari Wardoyo, Y., & Bhirini Slamet, A. (2022). The Urgency of Establishing Guidelines for Handling *Cybercrime* Cases in the Indonesian National Police Department. *KnE Social Sciences*, *2022*, 349–359. https://doi.org/10.18502/kss.v7i15.12107

Apriani, D., Munawar, K., & Setiawan, A. (2019). ALAT MONITORING PADA DEPO AIR MINUM BIRU CABANG NAGRAK KOTA TANGERANG MENGGUNAKAN AIR GALON BERBASIS SMS GATEWAY. *SENSI Journal*, *5*(1). https://doi.org/10.33050/sensi.v5i1.325

Arianto, A. R., & Anggraini, G. (2019). Building Indonesia'S National Cyber Defense and Security To Face the Global Cyber Threats Through Indonesia Security Incident Response Team on Internet Infrastructure (Id-Sirtii). *Jurnal Pertahanan & Bela Negara*, *9*(1), 17. https://doi.org/10.33172/jpbh.v9i1.515

Arikunto, S. (2010). *Prosedur Penelitian (Suatu Pendekatan Praktik)*. Rineka Cipta.

Arliman. S, L. (2019). MEWUJUDKAN PENEGAKAN HUKUM YANG BAIK DI NEGARA HUKUM INDONESIA. *Dialogia Iuridica: Jurnal Hukum Bisnis Dan Investasi*, *11*(1). https://doi.org/10.28932/di.v11i1.1831

Arwana, Y. C. (2022). Victims of Cyber Crimes in Indonesia : A Criminology and Victimology Perspective. *Semarang State University Undergraduate Law & Society Review*, *May*, 181–200. https://doi.org/10.15294/lsr.v2i2.53754

Chanda Halim, & Hendri Prasetyo. (2018). Penerapan Artificial Intelligence dalam Computer Aided Instructure(CAI). *Jurnal Sistem Cerdas*, *1*(1). https://doi.org/10.37396/jsc.v1i1.6

Damayanti, D., & Ismowati, M. (2021). The Implementation of The *Cybercrime* Prevention Policy at The Metro Jaya Police Station in Central Jakarta. *ICSTIAMI*, *July*, 17–18. https://doi.org/10.4108/eai.17-7-2019.2302054

Darmaningrat, E. W. T., Noor Ali, A. H., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi. *Sewagati*, *6*(2). https://doi.org/10.12962/j26139960.v6i2.92

Faridah, S. (2018). KEBEBASAN BERAGAMA DAN RANAH TOLERANSINYA. *Lex Scientia Law Review*, *2*(2). https://doi.org/10.15294/lesrev.v2i2.27585

Hartati, S., Karyono, H., & Karno Sabowo, H. (2022). Implementation of The Law on Information and Electronic Transactions and Pancasila Law Enforcement Related to *Cybercrimes* in Indonesia. *International Journal of Educational Research & Social Sciences*, *3*(1), 425–436. https://doi.org/10.51601/ijersc.v3i1.290

Keary, J. (2022). Rebuffing Russian Ransomware: How the United States Should Use the Colonial Pipeline and JBS USA Hackings as a Defense Guide for Ransomware. In *Seton Hall*.

Maltha, H. S., Suradinata, E., Djaenuri, M. A., & Lukman, S. (2019). Mitigating Strategy of Cyber Crime for Indonesian National Police. *International Journal of Recent Technology and Engineering*, *8*(3S2), 472–475. https://doi.org/10.35940/ijrte.c1105.1083s219

Mandasari Saragih, Y., & Utama Siahaan, A. P. (2016). Cyber Crime Prevention Strategy in Indonesia. *International Journal of Humanities and Social Science*, *3*(6), 22–26. https://doi.org/10.14445/23942703/ijhss-v3i6p106

Manihuruk, H., & Tarina, D. D. Y. (2020). State Defense Efforts through Strengthening Cyber Law in Dealing with Hoax News. *International Journal of Multicultural and Multireligious Understanding*, *7*(5), 27–36.

Mashdurohatun, A., Sidji, R., Gunarto, & Mahmutarom. (2017). Factors causing banking cyber crime in Indonesian. *International Journal of Economic Research*, *14*(15), 293–311.

Putra, A. K. (2016). Analisis Hukum Yurisdiksi Tindak Kejahatan Siber (*Cybercrime*) Berdasarkan Convention on *Cybercrime*. *Jurnal Ilmu Hukum*, *7*.

Rahmat, A. F., Mutiarin, D., Pribadi, U., & Rahmawati, E. (2022). Overseeing Cyber-Neighborhoods: How Far the Indonesian National Police Effort in Handling *Cybercrime*? *International Conference on Public Organization*, *209*(Iconpo 2021), 549–555.

Rais, M. A., & Songkarn, P. (2022). Hacker and the Treat for National Security: Challenges in Law Enforcement. *Indonesian Journal of Counter Terrorism and National Security*, *1*(1), 45–66. https://doi.org/10.15294/ijctns.v1i1.56728

Raodia, R. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (*Cybercrime*). *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum*, *6*(2). https://doi.org/10.24252/jurisprudentie.v6i2.11399

Rizal, M., & Yani, Y. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *JAS (Journal of ASEAN Studies)*, *4*(1), 61. https://doi.org/10.21512/jas.v4i1.967

Rosmaladewi, R., & Abduh, A. (2019). the Impact of Information Technology on Efl Teaching in Indonesia. *ELT Worldwide: Journal of English Language Teaching*, *6*(1), 21. https://doi.org/10.26858/eltww.v6i1.9802

Sakban, A., Kasmawati, A., & Tahir, H. (2020). The Implementation Repressive Method to Solving of Cyber-Bullyingin the West Nusa Tenggara Universitas Muhammadiyah Mataram , Mataram - Indonesia Universitas Negeri Makassar , Makassar - Indonesia. *International Journal of Advanced Science and Technology*, *29*(5), 13414–13421.

Saleh, G. S. (2022). Juridical Analysis of the Crime of Online Store Fraud in Indonesia. *Jurnal Hukum Dan Peradilan*, *11*(1), 151. https://doi.org/10.25216/jhp.11.1.2022.151-175

Sarre, R., Lau, L. Y. C., & Chang, L. Y. C. (2018). Responding to *Cybercrime*: current trends. *Police Practice and Research*, *19*(6), 515–518. https://doi.org/10.1080/15614263.2018.1507888

Setiawan, W. B. M., Churniawan, E., & Faried, F. S. (2020). UPAYA REGULASI TEKNOLOGI INFORMASI DALAM MENGHADAPI SERANGAN SIBER (CYBER ATTACK) GUNA MENJAGA KEDAULATAN NEGARA KESATUAN REPUBLIK INDONESIA. *JURNAL USM LAW REVIEW*, *3*(2). https://doi.org/10.26623/julr.v3i2.2773

Sugiartha, I. N. G., Dewi, S. L., & Widyantara, I. M. M. (2021). Law Enforcement Of Fraud Through Electronic Media. *Sociological Jurisprudence Journal*, *4*(1), 45–53.

Sugiharti, L., Esquivias, M. A., Shaari, M. S., Agustin, L., & Rohmawati, H. (2022). Criminality and Income Inequality in Indonesia. *Social Sciences*, *11*(3), 1–19. https://doi.org/10.3390/socsci11030142

Suhendi, D., & Asmadi, E. (2021). Cyber laws Related to Prevention of Theft of Information Related to Acquisition of Land and Infrastructure Resources in Indonesia. *International Journal of Cyber Criminology*, *15*(2), 135–143. https://doi.org/10.5281/zenodo.4766552

Wicaksono, I. A., & Najicha, F. U. (2021). Penerapan Asas Ultimum Remedium Dalam Penegakan Hukum Di Bidang Lingkungan Hidup. *Pagaruyuang Law Journal*, *5*(1). https://doi.org/10.31869/plj.v5i1.2828

Wijatmoko, T. E. (2021). Digital Forensic Readines Index (DiFRI) untuk Mengukur Kesiapan Penanggulangan *Cybercrime* pada Kantor Wilayah Kementerian Hukum dan HAM DIY. *Cyber Security Dan Forensik Digital*, *4*(1). https://doi.org/10.14421/csecurity.2021.4.1.2235.